Confidential

Subject: ISOC Blue Advisory – November 21, 2006 Excerpted from SANS Critical Vulnerabilities

Severity: Low

What: November 21, 2006 Excerpted from SANS Critical Vulnerabilities

Action: This is a notification from the ISOC for your information

Current Status: These are current as of 11/21/2006

ISOC Next Steps: If you have any questions please contact the ISOC.

Additional Information: November 21, 2006 Excerpted from SANS Critical Vulnerabilities

(1) CRITICAL: Microsoft Windows Workstation Service Buffer Overflow (MS06-070)
Affected:
Microsoft Windows 2000 SP4
Microsoft Windows XP SP2

Description: The Microsoft Windows Workstation Service, used to support inter-system communication (including file and printer sharing), contains a buffer overflow. By sending a specially-crafted request to the service, an attacker could take complete control of the vulnerable system. Technical details and several proofs-of-concept are available for this vulnerability. Users are advised to block ports ports 139 and 445 on both TCP and UDP at the network perimeter if possible.

Status: Microsoft confirmed, updates available.

Council Site Actions: All reporting council sites are responding to the majority of the Microsoft issues in the same manner. They plan to distribute the patches during their next regularly scheduled system maintenance window. They will expedite the process if exploits are released.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/bulletin/ms06-070.mspx
SecuriTeam Advisory (includes proof-of-concept)
http://www.securiteam.com/windowsntfocus/6V00D1PHFW.html
eEye Security Advisory
http://www.securityfocus.com/archive/1/451588
Proofs-of-Concept
http://downloads.securityfocus.com/vulnerabilities/exploits/MS06-070_exploit.txt
http://milw0rm.com/exploits/2809
http://milw0rm.com/exploits/2800
http://milw0rm.com/exploits/2789
Exploit Modules (Immunity Partners Program)
https://www.immunityinc.com/downloads/immpartners/ms06_070.tar
https://www.immunityinc.com/downloads/immpartners/ms06_070-2.tar

SecurityFocus BID
http://www.securityfocus.com/bid/20985

****

(2) CRITICAL: Microsoft XML Core Services XMLHTTP ActiveX Control Remote Code Execution (MS06-071)
Affected:
Microsoft XML Core Services versions 4.0 and 6.0

Description: Microsoft XML Core Services, Microsoft's implementation of various XML technologies, contains a remote code execution vulnerability in the XMLHTTP ActiveX control. A malicious web page that instantiates this control could execute arbitrary code with the privileges of the current user. Users can mitigate the impact of this vulnerability by disabling the vulnerable ActiveX controls via Microsoft's "kill bit" mechanism for CLSIDs "88d96a0a-f192-11d4-a65f-0040963251e5" and "88d969c5-f192-11d4-a65f-0040963251e5". This vulnerability is being actively exploited in the wild. This vulnerability was covered in a previous @RISK entry.

Status: Microsoft confirmed, updates available.

Council Site Actions: All reporting council sites are responding to the majority of the Microsoft issues in the same manner. They plan to distribute the patches during their next regularly scheduled system maintenance window. They will expedite the process if exploits are released.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/Bulletin/MS06-071.mspx
Microsoft Knowledge Base Article (details the "kill bit" mechanism)
http://support.microsoft.com/kb/240797
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=44#widely1
SecurityFocus BID
http://www.securityfocus.com/bid/20915

****

(3) CRITICAL: Microsoft Internet Explorer Multiple Vulnerabilities (MS06-067)
Affected:
Microsoft Windows 2000 SP4
Microsoft Windows XP SP2
Microsoft Windows 2003 SP0/SP1

Description: Microsoft Internet Explorer contains two vulnerabilities: (1) The DirectX DirectAnimation ActiveX control contains a memory corruption vulnerability. A malicious web page that instantiates this control could exploit this vulnerability. This vulnerability has been discussed in a previous issue of @RISK. Users can mitigate the impact of this vulnerability by disabling the vulnerable ActiveX control via Microsoft's "kill bit" mechanism for CLSID "D7A7D7C3-D47F-11D0-89D3-00A0C90833E6". (2) Failure to properly handle specially-crafted HTML code can lead to a memory corruption vulnerability. A specially-crafted web page could exploit this vulnerability. Exploiting ether vulnerability can lead to arbitrary code execution with the privileges of the current user. Technical details and proofs-of-concept for these exploits are available.

Status: Microsoft confirmed, updates available.

Council Site Actions: All reporting council sites are responding to the majority of the Microsoft issues in the same manner. They plan to distribute the patches during their next regularly scheduled system maintenance window. They will expedite the process if exploits are released.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/bulletin/ms06-067.mspx
Microsoft Knowledge Base Article (details the "kill bit" mechanism)
http://support.microsoft.com/kb/240797
Zero Day Initiative Advisory
http://www.zerodayinitiative.com/advisories/ZDI-06-041.html
Proof-of-Concept Exploit
http://downloads.securityfocus.com/vulnerabilities/exploits/19738.html
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=35#widely2
SecurityFocus BIDs
http://www.securityfocus.com/bid/21020
http://www.securityfocus.com/bid/19738

****

(4) CRITICAL: Microsoft Agent Buffer Overflow (MS06-068)
Affected:
Microsoft Windows 2000 SP4
Microsoft Windows XP SP2
Microsoft Windows 2003 SP0/SP1

Description: Microsoft Agent, a set of technologies used to enhance and manipulate the Microsoft Windows user interface, contains a buffer overflow. A specially-crafted web page that instantiates a vulnerable ActiveX control could exploit this vulnerability and execute arbitrary code with the privileges of the current user. It is believed to be also possible to exploit this vulnerability via specially-crafted ".ACF" file. Users can mitigate the impact of this vulnerability by disabling the vulnerable ActiveX controls via Microsoft's "kill bit" mechanisms for CLSIDs "D45FD31B-5C6E-11D1-9EC1-00C04FD7081F", F5BE8BD2-7DE6-11D0-91FE-00C04FD701A5", "4BAC124B-78C8-11D1-B9A8-00C04FD97575", "D45FD31D-5C6E-11D1-9EC1-00C04FD7081F", and "D45FD31E-5C6E-11D1-9EC1-00C04FD7081F".

Status: Microsoft confirmed, updates available.

Council Site Actions: All reporting council sites are responding to the majority of the Microsoft issues in the same manner. They plan to distribute the patches during their next regularly scheduled system maintenance window. They will expedite the process if exploits are released.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/bulletin/ms06-068.mspx
Microsoft Knowledge Base Article (details the "kill bit" mechanism)
http://support.microsoft.com/kb/240797
SecurityFocus BID
http://www.securityfocus.com/bid/21034

****

(5) CRITICAL: WinZip FileView ActiveX Control Remote Code Execution
Affected:
WinZip version 10.0 prior to build 7245

Description: WinZip, a popular archive utility for Microsoft Windows, contains a vulnerability in its FileView ActiveX control. A malicious web page that instantiates this control could exploit this vulnerability to execute arbitrary code with the privileges of the current user. Several exploits for this vulnerability are publicly available. Users can mitigate the impact of this vulnerability by disabling the vulnerable ActiveX control via Microsoft's "kill bit" mechanism for CLSID " A09AE68F-B14D-43ED-B713-BA413F034904". It is believed that installing Microsoft Security Update MS06-067 will also mitigate the impact of this vulnerability. There is a similar vulnerability in the Sky Software FileView ActiveX control; while these two controls are believed to be the same, it is unknown how the two vulnerabilities are related.

Status: WinZip confirmed, updates available.

Council Site Actions: most of the council sites are responding to this item. The patch for this item will be included in the rollout of the Microsoft patches. A few sites don't officially support this application and are relying on the user's auto-update feature to set the relevant kill bits.

References:
WinZip Change Log
http://www.winzip.com/wz7245.htm
Zero Day Initiative Advisory
http://www.zerodayinitiative.com/advisories/ZDI-06-040.html
Microsoft Knowledge Base Article (details the "kill bit" mechanism)
http://support.microsoft.com/kb/240797
SANS Internet Storm Center Handler's Diary Entry
http://isc.sans.org/diary.php?storyid=1861
Exploits
http://downloads.securityfocus.com/vulnerabilities/exploits/21060.html
http://downloads.securityfocus.com/vulnerabilities/exploits/prdelka-vs-MS-winzip.c
http://downloads.securityfocus.com/vulnerabilities/exploits/21060-2.html
http://milw0rm.com/exploits/2785
SecurityFocus BIDs
http://www.securityfocus.com/bid/21060
http://www.securityfocus.com/bid/21108

****

(6) MODERATE: Microsoft Client Service for NetWare Multiple Vulnerabilities (MS06-066)
Affected:
Microsoft Windows 2000 SP4
Microsoft Windows XP SP2
Microsoft Windows 2003 SP0/SP1

Description: Microsoft Windows Client Service for NetWare, used to provide access to Novell NetWare-accessible resources, contains multiple vulnerabilities: By sending specially-crafted messages to the service, an attacker could (1) exploit a buffer overflow in the service and execute arbitrary code on the system with SYSTEM privileges and (2) cause the system to stop responding. On Windows 2003 systems, attackers would require authentication to exploit these vulnerabilities. Additionally, the vulnerable service is not installed by default on any version of the vulnerable operating systems. Exploits for this vulnerability are available for Immunity CANVAS.

Status: Microsoft confirmed, updates available.

Council Site Actions: All reporting council sites are responding to the majority of the Microsoft issues in the same manner. They plan to distribute the patches during their next regularly scheduled system maintenance window. They will expedite the process if exploits are released.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/bulletin/ms06-066.mspx
Exploit Modules (Immunity Partners Program)
https://www.immunityinc.com/downloads/immpartners/ms06_066-1.tar
https://www.immunityinc.com/downloads/immpartners/ms06_066-2.tar
https://www.immunityinc.com/downloads/immpartners/ms06_066-3.tar
https://www.immunityinc.com/downloads/immpartners/ms06_066-4.tar
SecurityFocus BIDs
http://www.securityfocus.com/bid/21023
http://www.securityfocus.com/bid/20984

****

(7) MODERATE: Panda ActiveScan Multiple Vulnerabilities
Affected:
Panda ActiveScan version 5.53.00 and possibly prior

Description: Panda ActiveScan, a popular anti-spam and anti-malware solution, contains multiple vulnerabilities in included ActiveX components. A malicious web page that instantiates these ActiveX controls could exploit these vulnerabilities to execute arbitrary code with the privileges of the current user, disclose sensitive information, or reboot the victim's system.

Status: Panda confirmed, updates available.

References:
Secunia Advisory

http://www.securityfocus.com/archive/1/451864
Panda ActiveScan Home Page
http://www.pandasoftware.com/products/ActiveScan.htm
SecurityFocus BID
http://www.securityfocus.com/bid/21132

****

(8) MODERATE: Adobe Macromedia Flash Player Multiple Vulnerabilities (MS06-069)
Affected:
Microsoft Windows XP SP2

Description: Adobe Macromedia Flash Player, a popular player for rich web content, contains multiple vulnerabilities. This player is included with Microsoft Windows. These vulnerabilities include remote code execution, denial-of-service conditions, and the execution of arbitrary JavaScript. Note that, by default, Flash content is displayed automatically by most browsers. A fixed version of Flash Player was released by Adobe in September 2006. This issue is specifically for the version of Flash Player included by default with Microsoft Windows. These issues were discussed in a previous @RISK entry.

Status: Microsoft confirmed, updates available.

Council Site Actions: Most of the reporting council sites are responding to this item. They plan to distribute the patches during their next regularly scheduled system maintenance window. A few sites don't officially support this application and are investigating appropriate action, if any.

References:
Microsoft Security Bulletin
http://www.microsoft.com/technet/security/bulletin/ms06-069.mspx
Adobe Security Bulletin
http://www.adobe.com/support/security/bulletins/apsb06-11.html
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely2
SecurityFocus BID
http://www.securityfocus.com/bid/19980

****

****
Other Software
****

(9) HIGH: NetGear Wireless Drivers Multiple Vulnerabilities
Affected:
NetGear MA521nd5.SYS driver version 5.148.724.2003 and possibly prior
NetGear WG111v2.SYS driver version 5.1213.6.316 and possibly prior

Description: The NetGear MA521nd5.SYS and WG111v2.SYS device drivers, used to control NetGear wireless cards, contain buffer overflow vulnerabilities. By sending a specially-crafted 802.11 (WiFi) frame to a vulnerable system, an attacker could exploit these buffer overflows and take complete control of the vulnerable system. No authentication is required, and attackers need only be within wireless range of the vulnerable system. These drivers are primarily designed for Microsoft Windows systems, but they are believed to be compatible with the "NdisWrapper" cross-platform driver framework, making it possible to run these drivers under Linux (and possibly other operating systems) on the Intel platform. These vulnerabilities was discovered as part of a project to discover bugs in various operating systems' kernels. Working exploits are available for these vulnerabilities. These vulnerabilities are similar to one discovered for Broadcom wireless device drivers that was documented in a previous issue of @RISK.

Status: NetGear has not confirmed, no updates available.

References:
Month of Kernel Bugs Advisories
http://projects.info-pull.com/mokb/MOKB-18-11-2006.html
http://projects.info-pull.com/mokb/MOKB-16-11-2006.html
Metasploit Modules
http://metasploit.com/svn/framework3/trunk/modules/auxiliary/dos/wireless/netgear_ma521_rates.rb
http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/driver/netgear_wg111_beacon.rb
NetGear Home Page
http://www.netgear.com
Wikipedia Entry on Device Drivers
http://en.wikipedia.org/wiki/Device_Driver
NdisWrapper Home Page
http://ndiswrapper.sourceforge.net
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=45#widely1
SecurityFocus BIDs
http://www.securityfocus.com/bid/21175
http://www.securityfocus.com/bid/21126

****

(10) HIGH: D-Link A5AGU.SYS Wireless Driver Buffer Overflow
Affected:
D-Link A5AGU.SYS driver version 1.0.1.41 and possibly prior

Description: The D-Link A5AGU.SYS device driver, used to control D-Link wireless cards, contains a buffer overflow vulnerability. By sending a specially-crafted 802.11 (WiFi) frame to a vulnerable system, an attacker could exploit this buffer overflow and take complete control of the vulnerable system. No authentication is required, and attackers need only be within wireless range of the vulnerable system. This driver is primarily designed for Microsoft Windows systems, but it is believed to be compatible with the "NdisWrapper" cross-platform driver framework, making it possible to run this driver under Linux (and possibly other operating systems) on the Intel platform. This vulnerability was discovered as part of a project to discover bugs in various operating systems' kernels. Working exploits are available for this vulnerability. This vulnerability is similar to one discovered for Broadcom wireless device drivers that was documented in a previous issue of @RISK.

Status: D-Link has not confirmed, no updates available. Newer versions of the driver available with some cards appear to resolve this issue. Note that some reports have listed the driver as "ASAGU.SYS".

References:
Month of Kernel Bugs Advisory
http://projects.info-pull.com/mokb/MOKB-13-11-2006.html
Metasploit Module
http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/driver/dlink_wifi_rates.rb
D-Link Home Page
http://www.dlink.com
Wikipedia Entry on Device Drivers
http://en.wikipedia.org/wiki/Device_Driver
NdisWrapper Home Page
http://ndiswrapper.sourceforge.net
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=45#widely1
SecurityFocus BID
http://www.securityfocus.com/bid/21032

****

(11) MODERATE: Marshal MailMarshal ARJ Directory Traversal Vulnerability
Affected:
MailMarshal SMTP versions 5.x, 6.x and 2006
MailMarshal for Exchange 5.x

Description: Marshal MailMarshal, a popular product used to protect against email spam, malware, phishing, and other threats, contains a directory-traversal vulnerability when processing ARJ-compressed archives. Specially-crafted file names within these archives can cause the arbitrary creation of files on the server. It is not possible to delete or replace existing files. This vulnerability could be leveraged execute arbitrary code on the system by placing files in locations where it is known they will be executed. Some technical details for this vulnerability are publicly available.

Status: Marshal confirmed, updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Marshal Knowledge Base Article
http://www.marshal.com/kb/article.aspx?id=11450
Zero Day Initiative Advisory
http://www.zerodayinitiative.com/advisories/ZDI-06-039.html
Wikipedia Article on ARJ Compression
http://en.wikipedia.org/wiki/ARJ
Marshal Home Page
http://www.marshal.com
SecurityFocus BID
http://www.securityfocus.com/bid/20999

****

(12) MODERATE: PowerDNS Recursor Multiple Vulnerabilities
Affected:
PowerDNS versions prior to 3.1.4

Description: PowerDNS, a popular Domain Name System (DNS) server, contains multiple vulnerabilities in its recursor component: (1) By sending a specially-crafted request to the recursor, an attacker could exploit a buffer overflow and potentially execute arbitrary code with the privileges of the PowerDNS recursor process. (2) Sending a specially-crafted request to the recursor can cause the process to exhaust its allocated stack space and crash, leading to a denial-of-service condition. Because this product is open source, technical details for these vulnerabilities can be easily obtained via source code analysis.

Status: PowerDNS confirmed, updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
PowerDNS Security Advisories
http://doc.powerdns.com/powerdns-advisory-2006-01.html
http://doc.powerdns.com/powerdns-advisory-2006-02.html
PowerDNS Home Page
http://www.powerdns.com
SecurityFocus BID
http://www.securityfocus.com/bid/21037

****

(13) MODERATE: Grisoft AVG Anti-Virus Multiple Vulnerabilities
Affected:
AVG Anti-Virus versions prior to 7.1.407

Description: AVG Anti-Virus, a popular anti-virus system, contains multiple vulnerabilities. By sending a specially-crafted file through the system, an attacker could exploit these vulnerabilities to execute arbitrary code with the privileges of the anti-virus process. No technical details for these vulnerabilities are currently available.

Status: Grisoft confirmed, updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Grisoft Release Notes
http://www.grisoft.com/doc/36365/lng/us/tpl/tpl01
SecurityFocus BID
http://www.securityfocus.com/bid/21029

****

(14) LOW: Verity Ultraseek Multiple Vulnerabilities

Affected:
Ultraseek

Description: Ultraseek, a popular web search solution, contains multiple vulnerabilities. Attackers could exploit these vulnerabilities to bypass web proxy and other restrictions or disclose sensitive information. Authenticated users can also exploit these vulnerabilities to read arbitrary files on the server hosting Ultraseek.

Status: Ultraseek confirmed, updates available.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Ultraseek Release Notes
http://www.ultraseek.com/product_information/index.html
Zero Day Initiative Advisory
http://www.zerodayinitiative.com/advisories/ZDI-06-042.html
Ultraseek Home Page
http://www.ultraseek.com

Weekly Comprehensive List of Newly Discovered Vulnerabilities

Windows
06.46.1 CVE: CVE-2006-4688
Platform: Windows
Ref: http://www.microsoft.com/technet/security/Bulletin/MS06-066.mspx

06.46.2 CVE: CVE-2006-4691
Platform: Windows
Title: Microsoft Windows Workstation Service Remote Code Execution
Ref: http://www.microsoft.com/technet/security/Bulletin/MS06-070.mspx

06.46.3 CVE: CVE-2006-4687
Platform: Windows
Title: Microsoft Internet Explorer HTML Rendering Remote Code Execution
Ref: http://www.microsoft.com/technet/security/Bulletin/MS06-067.mspx

06.46.4 CVE: CVE-2006-4688,CVE-2006-4689
Platform: Windows
Title: Windows Client Service For Netware Remote Code Execution
Ref: http://www.microsoft.com/technet/security/Bulletin/MS06-066.mspx

06.46.5 CVE: CVE-2006-3445
Platform: Windows
Title: Microsoft Agent ActiveX Control Remote Code Execution
Ref: http://www.microsoft.com/technet/security/Bulletin/MS06-068.mspx

Third Party Windows Apps

06.46.6 CVE: Not Available
Platform: Third Party Windows Apps
Title: Infinicart Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21043

06.46.7 CVE: CVE-2006-5487
Platform: Third Party Windows Apps
Title: Marshal MailMarshal UNARJ Extraction Remote Directory Traversal
Ref: http://www.zerodayinitiative.com/advisories/ZDI-06-039.html

06.46.8 CVE: Not Available
Platform: Third Party Windows Apps
Title: Novell BorderManager ISAKMP Predictable Cookie
Ref: http://www.securityfocus.com/bid/21014

06.46.9 CVE: Not Available
Platform: Third Party Windows Apps
Title: Avahi Unauthorized Data Manipulation
Ref: http://www.securityfocus.com/bid/21016

06.46.10 CVE: Not Available
Platform: Third Party Windows Apps
Title: AVG Anti-Virus Multiple Remote Code Execution Vulnerabilities
Ref: http://www.securityfocus.com/bid/21029

06.46.11 CVE: CVE-2006-5198
Platform: Third Party Windows Apps
Title: WinZip ActiveX Control Remote Code Execution
Ref: http://www.winzip.com/wz7245.htm

06.46.12 CVE: Not Available
Platform: Third Party Windows Apps
Title: ASPIntranet Default.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21061

06.46.13 CVE: Not Available
Platform: Third Party Windows Apps
Title: Evolve Merchant Viewcart.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21070

06.46.14 CVE: Not Available
Platform: Third Party Windows Apps
Title: Conxint FTP Multiple Directory Traversal Vulnerabilities
Ref: http://www.securityfocus.com/bid/21081

06.46.15 CVE: Not Available

Platform: Third Party Windows Apps
Title: Teamtek Universal FTP Server Multiple Commands Remote Denial Of Service Vulnerabilities
Ref: http://www.securityfocus.com/bid/21085

06.46.16 CVE: Not Available
Platform: Third Party Windows Apps
Title: F-PROT Antivirus Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21086

06.46.17 CVE: Not Available
Platform: Third Party Windows Apps
Title: Eudora WorldMail Server Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21095

06.46.18 CVE: Not Available
Platform: Third Party Windows Apps
Title: Outpost Firewall PRO Multiple Local Denial of Service Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451672

06.46.19 CVE: Not Available
Platform: Third Party Windows Apps
Title: Biba Selenium Web Server Multiple Vulnerabilities
Ref: http://www.securityfocus.com/bid/21100

06.46.20 CVE: CVE-2006-3890
Platform: Third Party Windows Apps
Title: Sky Software FileView ActiveX Control Remote Code Execution Vulnerability
Ref: http://isc.sans.org/diary.php?storyid=1861
http://www.kb.cert.org/vuls/id/225217

06.46.21 CVE: Not Available
Platform: Third Party Windows Apps
Title: Mercury Mail Transport System Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21110

06.46.22 CVE: Not Available
Platform: Third Party Windows Apps
Title: Panda ActiveScan ActiveX Controls Multiple Remote Vulnerabilities
Ref: http://www.securityfocus.com/bid/21132

Mac OS

06.46.23 CVE: Not Available
Platform: Mac Os
Title: Apple Safari JavaScript Regular Expression Match Remote Denial of Service

Ref: http://www.securityfocus.com/archive/1/451542

Linux

06.46.24 CVE: CVE-2006-5778
Platform: Linux
Title: NetKit FTP Server ChDir Information Disclosure
Ref: http://www.securityfocus.com/bid/21000

06.46.25 CVE: Not Available
Platform: Linux
Title: Extremail Remote Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21084

06.46.26 CVE: Not Available
Platform: Linux
Title: Pragma Systems FortressSSH Unspecified Stack Buffer Overflow
Ref: http://www.securityfocus.com/bid/21106

HP-UX

06.46.27 CVE: Not Available
Platform: HP-UX
Title: HP Tru64 POSIX Threads Library Local Privilege Escalation
http://www1.itrc.hp.com/service/cki/docDisplay.do?admit=-682735245+1163704513944+28353475&docId=c008001

93

BSD

06.46.28 CVE: Not Available
Platform: BSD
Title: Multiple BSD Vendor FireWire IOCTL Local Integer Overflow
Ref: http://www.securityfocus.com/bid/21089

Unix

06.46.29 CVE: Not Available
Platform: Unix
Title: Chetcpasswd Multiple Vulnerabilities
Ref: http://www.securityfocus.com/bid/21102

06.46.30 CVE: Not Available
Platform: Unix
Title: Kerio WebStar Local Privilege Escalation
Ref: http://downloads.securityfocus.com/vulnerabilities/exploits/21123.pl

Cross Platform

06.46.31 CVE: Not Available
Platform: Cross Platform
Title: ProFTPD Unspecified Remote Code Execution
Ref: http://www.securityfocus.com/bid/20992

06.46.32 CVE: Not Available
Platform: Cross Platform

Title: D-Link DWL-G132 ASAGU.SYS Wireless Device Driver Stack Buffer Overflow
Ref: http://www.securityfocus.com/bid/21032

06.46.33 CVE: CVE-2006-4251, CVE-2006-4252
Platform: Cross Platform
Title: PowerDNS Remote Denial of Service and Buffer Overflow Vulnerabilities
Ref: http://doc.powerdns.com/powerdns-advisory-2006-01.html
http://doc.powerdns.com/powerdns-advisory-2006-02.html

06.46.34 CVE: Not Available
Platform: Cross Platform
Title: Sun Java Runtime Environment Information Disclosure
Ref: http://www.securityfocus.com/bid/21077

06.46.35 CVE: CVE-2006-5793
Platform: Cross Platform
Title: LibPNG Graphics Library PNG SET SPLT Remote Denial of Service
Ref: https://issues.rpath.com/browse/RPL-790

06.46.36 CVE: Not Available
Platform: Cross Platform
Title: Citrix Access Gateway Unspecified Information Disclosure
Ref: http://support.citrix.com/article/CTX111695

06.46.37 CVE: Not Available
Platform: Cross Platform
Title: Links ELinks SMBClient Remote Command Execution
Ref: http://www.securityfocus.com/bid/21082

06.46.38 CVE: Not Available
Platform: Cross Platform
Title: Kerio MailServer Remote Unspecified Denial of Service
Ref: http://www.securityfocus.com/bid/21091

Web Application

06.46.39 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Drake CMS Index.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/20998

06.46.40 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: IBM WebSphere FaultFactor Cross-Site Scripting
Ref: http://www.securiteam.com/windowsntfocus/6X00B0UHFE.html

06.46.41 CVE: Not Available

Platform: Web Application - Cross Site Scripting
Title: cPanel User and Dir Parameters Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21027

06.46.42 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Email Signature Script Unspecified Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21046

06.46.43 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: DirectAdmin Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21049

06.46.44 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Yetihost Helm Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21096

06.46.45 CVE: Not Available
Platform: Web Application - SQL Injection
Title: PHPKit Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451304

06.46.46 CVE: Not Available
Platform: Web Application - SQL Injection
Title: NuSchool CampusNewsDetails.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21006

06.46.47 CVE: Not Available
Platform: Web Application - SQL Injection
Title: NuCommunity Cl CatListing.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21015

06.46.48 CVE: Not Available
Platform: Web Application - SQL Injection
Title: NuRealestate Propertysdetails.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21017

06.46.49 CVE: Not Available
Platform: Web Application - SQL Injection
Title: BrewBlogger PrintLog.PHP SQL Injection
Ref: http://www.craigheffner.com/security/exploits/brewblogger1.3.1.txt

06.46.50 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ASP Scripter Products CPLogin.ASP SQL Injection Vulnerabilities

Ref: http://www.securityfocus.com/archive/1/451370

06.46.51 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ASP Portal Default1.ASP SQL Injection
Ref: http://www.securityfocus.com/archive/1/451384

06.46.52 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Munch Pro Switch.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21044

06.46.53 CVE: Not Available
Platform: Web Application - SQL Injection
Title: 20/20 Real Estate Listings.ASP SQL Injection
http://aria-security.net/advisory/Real%20Estate%20Listing%20System.txt

06.46.54 CVE: Not Available
Platform: Web Application - SQL Injection
Title: FunkyASP Glossary Glossary.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21055

06.46.55 CVE: Not Available
Platform: Web Application - SQL Injection
Title: SiteXpress E-Commerce System Dept.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21059

06.46.56 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Site Outlet E-Commerce Kit Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451771

06.46.57 CVE: Not Available
Platform: Web Application - SQL Injection
Title: DMXReady Site Engine Manager Index.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21064

06.46.58 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ASP Smiley Default.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21063

06.46.59 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Pilot Cart Pilot.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21065

06.46.60 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Megamail Product Review.PHP Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451300

06.46.61 CVE: Not Available
Platform: Web Application - SQL Injection
Title: CandyPress Store Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21090

06.46.62 CVE: Not Available
Platform: Web Application - SQL Injection
Title: High Performance Computers Solutions Shopping Cart Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451595

06.46.63 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Dragon Event Listing Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21098

06.46.64 CVE: Not Available
Platform: Web Application - SQL Injection
Title: WWWeb Cocepts CactuShop Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21076

06.46.65 CVE: Not Available
Platform: Web Application - SQL Injection
Title: BPG Multiple Products Vjob Parameter SQL Injection
Ref: http://www.securityfocus.com/bid/21094

06.46.66 CVE: Not Available
Platform: Web Application - SQL Injection
Title: I Systems UK Estate Agent Manager Default.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21103

06.46.67 CVE: Not Available
Platform: Web Application - SQL Injection
Title: ASPIntranet Mutiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21105

06.46.68 CVE: Not Available
Platform: Web Application - SQL Injection
Title: 20/20 Data Shed Listings.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21109

06.46.69 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Aspmforum Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21113

06.46.70 CVE: Not Available
Platform: Web Application - SQL Injection
Title: I-Gallery Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21122

06.46.71 CVE: Not Available
Platform: Web Application - SQL Injection
Title: BlogTorrent Preview Announce.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21125

06.46.72 CVE: Not Available
Platform: Web Application
Title: PHPJobscheduler Multiple Remote File Include Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451360

06.46.73 CVE: Not Available
Platform: Web Application
Title: RoundCube Webmail index.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21042

06.46.74 CVE: Not Available
Platform: Web Application
Title: ContentNow Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21024

06.46.75 CVE: Not Available
Platform: Web Application
Title: Samedia LandShop LS.PHP Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/20989

06.46.76 CVE: Not Available
Platform: Web Application
Title: ExoPHPdesk Pipe.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21003

06.46.77 CVE: Not Available
Platform: Web Application
Title: WordPress Functions.PHP Remote File Include
Ref: http://www.securityfocus.com/archive/1/451311

06.46.78 CVE: Not Available
Platform: Web Application

Title: ShopSystems Index.PHP SQL Injection
Ref: http://www.securityfocus.com/bid/21005

06.46.79 CVE: Not Available
Platform: Web Application
Title: phpManta View-Sourcecode.PHP Local File Include
Ref: http://www.securityfocus.com/bid/21008

06.46.80 CVE: Not Available
Platform: Web Application
Title: Rama CMS Lang Parameter Local File Include
Ref:
http://downloads.securityfocus.com/vulnerabilities/exploits/rama_poc.txt

06.46.81 CVE: Not Available
Platform: Web Application
Title: PHPWCMS Wcs User Lang Local File Include
Ref: http://www.milw0rm.com/exploits/2758

06.46.82 CVE: Not Available
Platform: Web Application
Title: NuStore Products.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21019

06.46.83 CVE: Not Available
Platform: Web Application
Title: ELOG Web Logbook ELogD Server Denial Of Service
Ref: http://www.securityfocus.com/bid/21028

06.46.84 CVE: Not Available
Platform: Web Application
Title: Phpdebug Debug test.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21047

06.46.85 CVE: Not Available
Platform: Web Application
Title: Bitweaver Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/20988

06.46.86 CVE: Not Available
Platform: Web Application
Title: XLineSoft PHPRunner PHPRunner.INI Local Information Disclosure
Ref: http://www.securityfocus.com/bid/21054

06.46.87 CVE: Not Available
Platform: Web Application
Title: AlTools ALFTP Authentication Bypass And Information Disclosure Vulenrabilities

Ref: http://www.securityfocus.com/bid/21058

06.46.88 CVE: Not Available
Platform: Web Application
Title: Plesk Multiple HTML Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21067

06.46.89 CVE: Not Available
Platform: Web Application
Title: PHPPeanuts Inspect.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21057

06.46.90 CVE: Not Available
Platform: Web Application
Title: Inventory Manager Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21069

06.46.91 CVE: Not Available
Platform: Web Application
Title: MGInternet Property Site Manager Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21073

06.46.92 CVE: Not Available
Platform: Web Application
Title: Dotdeb PHP PHP Self Path Info Email Header Injection
Ref: http://www.securityfocus.com/archive/1/451528

06.46.93 CVE: Not Available
Platform: Web Application
Title: Netvios Page.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21088

06.46.94 CVE: Not Available
Platform: Web Application
Title: Eudora WorldMail Server Remote Unspecified Denial of Service
Ref: http://www.securityfocus.com/bid/21099

06.46.95 CVE: Not Available
Platform: Web Application
Title: Nucleus CMS Unspecified HTML Injection
Ref: http://www.securityfocus.com/bid/21104

06.46.96 CVE: Not Available
Platform: Web Application
Title: Hot Links Perl PHP Information Disclosure
Ref: http://www.securityfocus.com/bid/21112

06.46.97 CVE: Not Available
Platform: Web Application
Title: BaalAsp Forum Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21111

06.46.98 CVE: Not Available
Platform: Web Application
Title: Extreme CMS Multiple HTML Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21116

06.46.99 CVE: Not Available
Platform: Web Application
Title: Extreme CMS Options.PHP Authentication Bypass
Ref: http://www.securityfocus.com/bid/21118

06.46.100 CVE: CVE-2006-5819
Platform: Web Application
Title: Verity Ultraseek Information Disclosure and Request Proxying Vulnerabilities
Ref: http://www.securityfocus.com/bid/21120

06.46.101 CVE: Not Available
Platform: Web Application
Title: Blog:CMS Dir Plugins and Dir Libs Multiple Remote File Include Vulnerabilities
Ref: http://www.securityfocus.com/bid/21124

06.46.102 CVE: Not Available
Platform: Web Application
Title: Odysseus Blog Blog.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/bid/21128

Citrix

06.46.103 CVE: Not Available
Platform: Network Device
Title: Citrix Access Gateway Advanced Access Control Multiple Vulnerabilities
Ref: http://support.citrix.com/article/CTX111614
http://support.citrix.com/article/CTX111615

Network Device

06.46.104 CVE: Not Available
Platform: Network Device
Title: XTACACS Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21107

Hardware

06.46.105 CVE: Not Available
Platform: Hardware
Title: Digipass Go3 Insecure Encryption

```
Ref: http://www.securityfocus.com/bid/21040
```

Thank you,
Information Security Operations Center (ISOC)
isoc@state.co.us
(303) 866-3465

E-MAIL NOTICE: This e-mail message (and any attachments) contains information belonging to the sender, which is confidential and legally privileged. If you are not the intended recipient, you are hereby notified that any disclosure, coping or distribution of this information or any action taken in reliance on the information within this email is strictly prohibited. If you have received this e-mail in error, please notify the sender and then delete the message (and any attachments) from your computer. Thank You.
*"Information Security - Working Together to Make **IT** happen"*